GSA Enterprise-Level
Cyber-Supply Chain Risk Management (C-SCRM)
Strategic Plan

Version 1.3
March 29, 2021

Executive Summary

GSA recognizes that every part of the agency is operating in a world of ever increasing supply chain risks as it relies more on information and communications technology (ICT),[1] and as adversaries become more sophisticated. To manage supply chain risks,[2] GSA must act as an enterprise to prioritize its investments in the integrity, quality, security, and resilience of its supply chains and of the products and services it procures, delivers, sells, and uses.

This Enterprise-Level Cyber-Supply Chain Risk Management (C-SCRM) Strategic Plan (plan) is intended to communicate GSA's commitment to continuously improving and strengthening its security posture and its strategy for addressing cyber supply chain risks.[3] Even though GSA already has a robust information technology (IT) governance scheme, it must continually be updated to address the changing and growing nature of supply chain risks, including cyber supply chain risks. GSA's existing formal information security program is managed by GSA IT and is consistent with the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) policy, and National Institute of Standards and Technology (NIST) guidelines. GSA IT develops policy for and conducts security assessments of GSA's internal and Government-wide IT systems, regardless of whether the system is managed by GSA or by a contractor. Additionally, GSA's Federal Acquisition Service (FAS) and Public Buildings Service

---

[1] Information and Communications Technology (ICT) is: (1) information technology as defined in 40 U.S.C. § 11101; (2) information system(s), as defined in section 44 U.S.C. § 3502; and (3) telecommunications equipment and telecommunications service(s) as those terms are defined in section 3 of the Communications Act of 1934 (47 U.S.C. § 153).

[2] Supply Chain Risk is the risk that any person may sabotage, maliciously introduce unwanted function, extract data, or otherwise manipulate the design, integrity, manufacturing, production, distribution, installation, operation, maintenance, disposition, or retirement of covered articles so as to surveil, deny, disrupt, or otherwise manipulate the function, use, or operation of the covered articles or information stored or transmitted on the covered articles. 41 U.S.C. § 4713.

[3] SCRM is the management of risk to the integrity, trustworthiness, and authenticity of products and services within the supply chain. It addresses the activities of foreign intelligence entities and any other adversarial attempts aimed at compromising the Government's supply chain. A subset of SCRM is "Cyber-SCRM" (C-SCRM), which is the process of identifying, assessing, preventing, and mitigating the risks associated with the distributed and interconnected nature of Information and Communications Technology (ICT) product and service supply chains. C-SCRM covers the entire life cycle of ICT (including design, development, distribution, deployment, acquisition, maintenance, and destruction). *See* Intelligence Community Directive 731, *Supply Chain Risk Management* (Dec. 7, 2013); NIST website, *Cyber Supply Chain Risk Management*.

(PBS) both strive to provide secure Government-wide and agency-facing offerings (i.e., products, services, and real estate), which are further outlined in supplemental FAS and PBS SCRM plans.[4] Along with leading Government-wide policy efforts, GSA's Office of Government-wide Policy (OGP) also coordinates GSA's enterprise-level SCRM program. GSA IT, FAS, PBS, and OGP are supported in these roles by GSA's other Staff Offices. Key positional and organizational roles and responsibilities for each of GSA's major Service and Staff Offices are included in Appendix A: Roles and Responsibilities.

GSA has synthesized this feedback into the following three strategic objectives, planned for Fiscal Years 2021-22:

(1) Address GSA's Highest Enterprise-Level Supply Chain Risks
(2) Further Mature GSA's Acquisition Workforce's Awareness of and Capabilities to Manage Supply Chain Risks
(3) Standardize GSA's Key Operational (Tier 2) C-SCRM Plans

Adopting these three strategic objectives will solidify how GSA's oversight and adherence to GSA IT policies and contracting policies provide the basis by which GSA assesses, responds to, and monitors ICT supply chain risks across the life cycle of ICT products and services.

Purpose and Focus

The purpose of this plan is to provide a strategic roadmap for implementing effective C-SCRM capabilities and practices within GSA. This plan contains three strategic objectives that span the scope of GSA's mission responsibilities and reflect a phased, achievable strategic approach that will ensure successful implementation and effectiveness of C-SCRM efforts across GSA and also advance Government-wide C-SCRM improvements.

According to NIST, there are three tiers into which C-SCRM should be integrated: organizational (enterprise-level), mission/business process (operational), and information system.[5]

[4] FAS Supply Chain Risk Management Organizational Level Plan (Apr. 30, 2019); FAS Supply Chain Risk Management Mission Level Plan (July 27, 2020); PBS Supply Chain Risk Management Organizational Level Plan (Jan. 25, 2021).
[5] NIST SP 800-161 (Apr. 2015).

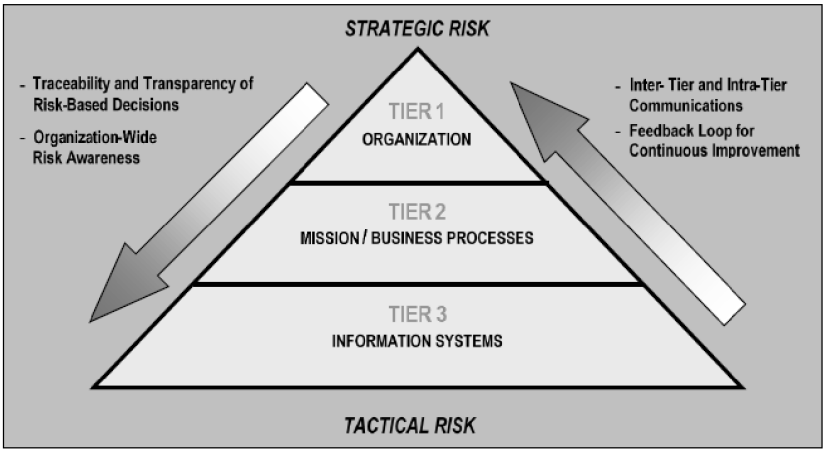

Figure 1: Multi-tiered Organization-wide Risk Management

This plan focuses on the integration of C-SCRM at GSA's organizational (enterprise) level, discussing the core functions, roles and responsibilities, and the approach GSA will take to implement C-SCRM controls, processes, governance, and compliance across the agency. To date, GSA has taken some actions at both the enterprise and business line levels, including the creation of some Tier 2 plans. Tier 2 plans are focused on subcomponent organizations or programs within GSA (e.g., FAS' and PBS' SCRM plans, linked in footnote 4, are Tier 2 plans) and Tier 3 plans will address system-level C-SCRM controls. Both Tier 2 and Tier 3 plans will include metrics, as appropriate.

According to the Government Accountability Office (GAO), there are seven foundational areas for managing ICT supply chain risks, and GSA is deficient in six of the seven C-SCRM foundational practices.[6]

The focus of this plan is intentionally targeted toward establishing a core foundational capability identified by NIST and GAO that GSA can expand and mature over time. These baseline functions include the ability to assess and make risk-based decisions when acquiring ICT products and services and to ensure that GSA integrates C-SCRM considerations into its contracts and system controls.

This plan also recognizes the dependencies on Government-wide planning efforts, processes, and decisions that are currently in process. As Government-wide policy direction, process guidance, and requirements are clarified and communicated, GSA will update and refine its strategy and operational implementation plans and actions.

[6] *Information and Communications Technology: Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks* (GAO-21-164SU) (Oct. 27, 2020). This report has been labeled "controlled unclassified information" and has not been publicly released. By footnote, GAO agreed that GSA had completed the first recommendation by, among other things, creating the GSA SCRM Executive Board. *See id.*, at 18 n.a, 19 n.38, 63 n.a, 81 n.1.

Background

The Federal Acquisition Supply Chain Security Act of 2018 requires all Executive Branch agencies to establish a formal SCRM program and to conduct supply chain risk assessments.[7] The law also requires GSA to take actions to provide better assurance that the products, services, and solutions it offers and provides to its customer agencies appropriately address supply chain risks.[8]

As a member of the Federal Acquisition Security Council (FASC), which was created by the Federal Acquisition Supply Chain Security Act of 2018, GSA has an instrumental role in the development and implementation of a Government-wide SCRM framework. As such, GSA is assisting the FASC in its work to develop and promulgate guidance to agencies and to recommend exclusion or removal of high-risk suppliers and products. GSA's Government-wide role extends beyond its FASC membership as it is well-positioned to drive positive change across the Federal landscape through its many customer-agency-facing business lines and via the leadership and support it provides to enable and facilitate interagency engagement.

GSA's enterprise-level C-SCRM program relies heavily on GSA IT's already robust IT governance scheme and acquisition policy issued by GSA's Chief Acquisition Officer and Senior Procurement Executive. Additionally, FAS has issued two Tier 2 plans and PBS has drafted its Tier 2 plan, which help secure GSA's Government-wide and agency-facing offerings (i.e., products, services, and real estate).

To unify GSA's approach to SCRM, the Administrator of General Services established a cross-functional GSA SCRM Executive Board to lead GSA-wide SCRM activities.[9] The SCRM Executive Board is an executive team that prioritizes and develops policies and processes and provides oversight to ensure a harmonized approach for SCRM activities GSA-wide. It is chaired by the Chief Acquisition Officer and its members are the Chief Information Officer, the Chief Information Security Officer, the Chief Privacy Officer, the Chief Financial Officer, the Chief Administrative Services Officer, the Commissioner of FAS, the Commissioner of PBS, the Associate Administrator for Mission Assurance, the General Counsel, and representatives of the Office of the Administrator, the Office of Congressional and Intergovernmental Affairs, and the Office of Strategic Communication.

The Board established a GSA-wide Working Group to further develop GSA's SCRM strategy and to ensure that the SCRM Executive Board has the information necessary to make informed risk-management decisions. From a preliminary review of the current

---

[7] The Federal Acquisition Supply Chain Security Act of 2018 is Title II of the SECURE Technology Act (P.L. 115-390) (Dec. 21, 2018).

[8] For example, when the FASC issues Government-wide exclusion orders, GSA "shall help facilitate implementation of such [exclusion]orders by removing the covered articles or sources identified in the orders from such contracts" (e.g. GSA Government-wide offerings). 41 USC §1323(c)(5)(C).

[9] GSA Supply Chain Risk Management (SCRM) Executive Board (June 1, 2020).

state of Government-wide SCRM requirements, GSA Staff or Service Offices' ongoing SCRM initiatives, and GSA's readiness, the Working Group is aware of numerous ongoing activities addressing SCRM across GSA.

Additional working groups and working meetings of the SCRM Executive Board include the SCRM Review Board, a cross-agency, interdisciplinary team that provides SCRM-related guidance and implementation decisions to GSA's acquisition workforce, monthly cross-agency meetings on SCRM policy initiatives and financial and budgetary planning for SCRM, and ad hoc meetings (previously, these meetings were weekly) focused on implementing Section 889 of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019.

To further mature GSA's C-SCRM program, this plan identifies three strategic objectives:

(1) Address GSA's Highest Enterprise-Level Supply Chain Risks
(2) Further Mature GSA's Acquisition Workforce's Awareness of and Capabilities to Manage Supply Chain Risks
(3) Standardize GSA's Key Operational (Tier 2) C-SCRM Plans

Adopting these three strategic objectives will solidify how GSA's oversight and adherence to GSA IT policies and contracting policies provide the basis by which GSA identifies, assesses, responds to, and monitors ICT supply chain risks across the life cycle of ICT products and services.

Strategic Objective 1: Address GSA's Highest Enterprise-Level Supply Chain Risks

The SCRM Executive Board provides enterprise-level management of GSA's SCRM program by prioritizing and developing policies, processes, and oversight to ensure a harmonized approach for SCRM activities across GSA. Key positional and organizational roles and responsibilities for the SCRM Executive Board and each of GSA's major Service and Staff Offices are included in Appendix A: Roles and Responsibilities.

GSA mitigates risk by using basic controls set forth in GSA's existing formal information security program, consistent with FISMA, OMB policy, and NIST guidelines. For example, GSA requires system security plans and assesses those plans every three years through the Assessment and Authorization (A&A, formerly Authorization to Operate (ATO)) process. GSA simplified and consolidated numerous GSA IT security requirements into a single guide for GSA IT personnel and acquisition workforce (CIO-IT Security-09-48), which requires adherence to GSA's A&A process, as identified

in CIO-IT Security-06-30, Managing Enterprise Cybersecurity Risk.[10] CIO-IT Security-06-30 defines how GSA assesses, responds to, and monitors ICT supply chain risks for GSA information systems across the life cycle of ICT products and services. GSA IT is in the process of updating CIO-IT Security-06-30, Managing Enterprise Cybersecurity Risk, CIO-IT Security-09-48, Security and Privacy Requirements for IT Acquisition Efforts, and other procedural guides and templates to, among other things, incorporate updated guidance and requirements from NIST (specifically NIST Special Publication (SP) 800-53, rev. 5). Updated versions of these two guides will be published by April 15, 2021. SCRM assessments required by these and other GSA IT policies will be used by GSA IT and the SCRM Executive Board to conduct GSA-wide risk assessments.

GSA accepts that supply chain risks will never be completely eliminated, that budgets are limited, and that it must prioritize its efforts. Therefore, in accordance with its risk tolerance, GSA, is first emphasizing addressing and reducing supply chain risks for GSA's four IT systems that are categorized by FISMA as "high impact."[11] GSA will review the current SCRM requirements (e.g., adherence to CIO-IT Security-09-48) and the flexibility to add new SCRM requirements (e.g., the soon-to-be-updated version of CIO-IT Security-09-48 and NIST SP 800-53, rev. 5) for these four "high impact" systems.

GSA's next priority is its "moderate impact" systems that are used across the Government.[12] Management (both internal controls and relevant contracts) of these Government-wide, "moderate impact" systems will be reviewed next by GSA IT, with assistance from FAS and OGP, to ensure full compliance with GSA's current SCRM requirements (e.g., adherence to CIO-IT Security-09-48) and the flexibility to add new SCRM requirements by May 31, 2021. Additionally, GSA IT plans to accelerate NIST SP 800-53 rev. 5's requirement for an independent third-party security assessment of each Government-wide "moderate impact" system's SCRM controls in its update to CIO-IT

---

[10] IT Security Procedural Guide: Managing Enterprise Cybersecurity Risk (CIO-IT Security-06-30, rev. 18) (Sept. 11, 2020); IT Security Procedural Guide: Security and Privacy Requirements for IT Acquisition Efforts (CIO-IT Security-09-48, rev. 5) (Aug. 25, 2020).

[11] GSA's four "high impact" systems are: (1) AT&T Managed Trusted Internet Protocol Services (MTIPS); (2) CenturyLink MTIPS; (3) Verizon MTIPS; and (4) USAAccess. System categorization is governed by FISMA and the Standards for Security Categorization of Federal Information and Information Systems (NIST Federal Information Processing Standards Publication (FIPS PUB) 199).

[12] GSA's 23 Government-wide, "moderate impact" systems are: (1) AT&T Business Support System (ATT BSS); (2) AT&T Operational Support System (ATT OSS); (3) BT Federal Business Support System; (4) CenturyLink Operational Support System; (5) Core Tech Business Support System (CBSS); (6) DigiCert PKI Shared Service Provider (DCPKI SSP); (7) e-Gov Travel - Concur Government Edition (eGT CGE); (8) e-Gov Travel - e2Solutions (eGT e2S); (9) Entrust PKI Shared Service Provider (ETPKI SSP); (10) Federal Public Key Infrastructure (FPKI); (11) Granite Business Support System (GBSS); (12) Harris Business Support System (HBSS); (13) Level 3 Networx OSS/CTL EIS BSS; (14) Login.gov; (15) MetTel Business Support System (MTBSS); (16) MicroTech BSS; (17) SmartPay - Citibank; (18) SmartPay - US Bank; (19) System for Award Management (SAM); (20) Verizon Business Support System; (21) Verizon Operational Support System; (22) Verizon PKI Shared Service Provider (VZPKI SSP); and (23) WidePoint PKI Shared Service Provider (WPPKI SSP).

Security-09-48.[13] Updates for system security plans are anticipated by September 30, 2021. GSA IT anticipates that these controls will be implemented, assessed, and each system re-authorized by March 31, 2022.

GSA will turn to reviewing its remaining IT systems in the future.

Lastly, in partnership with the Office of Strategic Communication, OGP, GSA IT, FAS, PBS, and the rest of GSA, the SCRM Executive Board will ensure that GSA's SCRM efforts and plans are clearly communicated to internal and external stakeholders following creation of and using the GSA C-SCRM journey map (see Strategic Objective #2).

Strategic Objective 2: Further Mature GSA's Acquisition Workforce's Awareness of and Capabilities to Manage Supply Chain Risks

GSA mitigates risk by using basic controls set forth in the Federal Acquisition Regulation (FAR). For example, acquisition plans address key risk areas, offerors make representations and certifications that certain supply chain risks are addressed as part of their proposals and are vetted for responsibility prior to award, and key standard terms are included in GSA contracts. Any GSA-specific acquisition policies that supplement or deviate from the requirements in the FAR will be issued by the GSA Senior Procurement Executive. In recognition of the risk to GSA, the SCRM Executive Board asked the Senior Procurement Executive to consider establishing GSA-specific acquisition policies without waiting for the publication of Government-wide regulations and policies.

To further understand GSA's current C-SCRM skills, awareness, capabilities, and associated gaps, OGP, in partnership with FAS' Technology Transformation Service, will create a GSA C-SCRM journey map that will be used to raise awareness of C-SCRM among GSA's acquisition workforce (e.g., contracting officers, contracting officer's representatives, project managers). The journey map will also be an ongoing resource for GSA's acquisition workforce as it will breakdown C-SCRM considerations during various milestones throughout the acquisition life cycle. Using a human-centered design process, the journey map will be based on insights gathered from a diverse set of GSA acquisition workforce members across Service and Staff Offices. GSA will leverage information identified in the journey map process and develop or identify workforce training to further invest in long-term GSA acquisition workforce SCRM skills, resulting in an acquisition workforce that is better equipped to address supply chain risks with additional training, certifications, and learning programs across function areas and program offices related to SCRM, including C-SCRM.

[13] CIO-IT Security-09-48, as updated, will accelerate the third-party security assessment of incorporation of the new controls for GSA's four "high impact" systems as well.

Existing internal-GSA procedures require GSA IT reviews of all new procurements involving GSA information systems for, among other things, proper incorporation of IT security considerations and controls.[14] All of GSA, including GSA IT, FAS, PBS, OGP, and the Office of Mission Assurance (OMA) continually updates its security policies, considerations, and controls as Government-wide guidance is published and new threats are discovered.

To assist GSA's acquisition workforce with vetting GSA's suppliers, GSA developed sample language for contracting officers to include in solicitations. These sample SCRM documents can be tailored or used as part of the statement of work to require offerors to address supply chain risks.[15]

The GSA Acquisition Manual (GSAM) provides information on how to manage supply chain risks for contractor-managed GSA systems.[16] Specifically, contracting officers are required to submit a supply chain event report based on offerors' disclosures before contracts are awarded or if a "prohibited article" (including a counterfeit or compromised ICT product) is discovered within the supply chain of an existing contract.[17] Supply chain event reports are reviewed by GSA's SCRM Review Board, a cross-agency, interdisciplinary working group of the SCRM Executive Board. OGP is currently in the process of updating the GSAM to, among other things, incorporate relevant portions of Acquisition Letter MV-20-10 and include pre-award SCRM procedures. A rule to update the GSAM is anticipated by December 31, 2021 (Case 2021-G512).

GSA IT is already in the process of updating CIO-IT Security-09-48 to include, among other things, GSA-specific organizational ICT SCRM requirements for inclusion in contracts that are tailored to the type of contract and business needs. The updated CIO-IT Security-09-48 is expected to be published by April 15, 2021.

In an example of conducting GSA-wide security and risk assessments in accordance with CIO-IT Security-09-48, the SCRM Executive Board will also decide whether existing supply chain risks warrant the creation of GSA-specific language before related Government-wide requirements are published.[18] Regardless of the SCRM Executive Board's pre-Government-wide-requirements risk assessment, following publication of

---

[14] *See* Contract Requirements for GSA Information Systems (Acquisition Letter MV-19-04) (Jan. 3, 2019) at 3.
[15] See insite.gsa.gov/scrm.
[16] *See* GSAM Subpart 504.70.
[17] *See* Workforce Guidance on FY2019 NDAA Section 889 "Part B" (Acquisition Letter MV-20-10) (Aug. 13, 2020) at 5; GSAM 504.7005(a).
[18] GSA is aware of multiple pending Government-wide requirements, including FAR Case 2017-013 "Breaches of Personally Identifiable Information," FAR Case 2018-017 "Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment," FAR Case 2019-009 "Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment", and a Final Rule from the FASC regarding, among other things, information sharing (the related Interim Final Rule (85 FR 54263) was published on September 1, 2020).

Government-wide requirements, GSA will adopt GSA-specific requirements as necessary.

OGP and GSA IT establish GSA's acquisition and IT policies, and FAS and PBS are charged with following those requirements. To assist in leadership of their SCRM programs, FAS and PBS have named supply chain leads for their respective organizations and are engaging in awareness and training programs, as well as identifying critical risks in their portfolios.

To further understand the SCRM capabilities of GSA's vendors, GSA will assess different approaches to ensuring that vendors comply with mandated SCRM requirements, such as NIST SP 800-171. In limited circumstances, GSA IT will require, as appropriate, third-party, independent assessments of non-IT vendors.

To secure its own supply chain and as part of its Government-wide responsibilities, GSA is monitoring the new Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC) program to determine whether GSA should leverage DoD's contractors' self assessments within DoD's Supplier Performance Risk System (SPRS), adopt elements of CMMC for GSA vendors, or create a GSA-specific approach. GSA is also exploring updates and changes to GSA's Government-wide acquisition vehicles.

Strategic Objective 3: Standardize GSA's Key Operational (Tier 2) C-SCRM Plans

GSA IT, FAS, and PBS have made significant strides in their management of ongoing supply chain risks of GSA's four key operational C-SCRM activities: detecting counterfeit and compromised ICT products, responding to C-SCRM incidents and sharing C-SCRM information, adding C-SCRM to cloud services, and addressing C-SCRM for drones.[19]

Detecting Counterfeit and Compromised ICT Products: Again, GSA IT is in the process of updating CIO-IT Security-09-48 and other GSA IT policies to, among other things, incorporate NIST SP 800-53, rev. 5. GSA will prioritize assessing controls for GSA's "high impact" and Government-wide, "moderate impact" systems, including a control for detecting counterfeit and compromised ICT products prior to their deployment. Updates for system security plans are anticipated by September 30, 2021. GSA IT anticipates that new controls will be implemented, assessed, and each system will be re-authorized by March 31, 2022. In addition, as part of an operational SCRM program, GSA has a need for risk-based, on-demand device testing to detect potential counterfeit or compromised products. It is outside of GSA's current technical expertise to perform low-level integrity tests, and the use of a third party service is needed. GSA IT is aiming to complete a pilot of this capability by September 30, 2021. Further operationalizing of this is contingent on new funding.

[19] The SCRM Executive Board will edit the list of GSA's key operational C-SCRM activities as necessary.

GSA maintains several internal controls to combat counterfeit or modified ICT products being offered through GSA's Government-wide contracts (e.g., Federal Supply Schedule contracts). For example, GSA uses software to aggregate and normalize contractors' catalogue data submitted to GSA and to flag high risk items (e.g., by questioning the origin of manufacturing, flagging low outlier pricing, identifying prohibited products such as those made by Kaspersky Labs). GSA also uses automation to remove noncompliant items from products and services from GSA's offerings.

Additionally, FAS and GSA IT have, in partnership with DoD, begun piloting a vendor risk assessment tool to illuminate ICT supply chains for select critical programs, including GSA's four "high impact" systems, contractors related to GSA's Enterprise Infrastructure Solutions (EIS) and 2nd Generation Information Technology (2GIT) contracts , and selected Federal Risk and Authorization Management Program (FedRAMP) products and systems. This pilot will be complete in late 2021 and appropriate next steps will be taken following its completion.

Responding to C-SCRM Incidents and Sharing C-SCRM Information: Several Government-wide policies outlining new requirements for agencies to share SCRM information are currently being drafted by the FASC and FAR Council. GSA, as a member of both, is working to share supply chain risk information across the Government, and OGP is developing procedures for sharing GSA supply chain risk information with the FASC. GSA is committed to sharing supply chain risk information across the Government and with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency.[20]

A key subset of information that must be shared by and with GSA is information gathered in relation to supply chain incidents. In accordance with applicable policies, GSA will share information about GSA-identified supply chain incidents and GSA's response to them. GSA will also receive information from other organizations (e.g., the intelligence community, contractors) about other supply chain incidents and will identify and mitigate any risks presented in that information. GSA IT will establish policies to coordinate C-SCRM incident response for GSA IT systems by March 31, 2021. FAS and PBS are also working to mature their C-SCRM incident response capabilities.

For its contracts, GSA has an established process for coordinating and resolving the discovery of prohibited articles. GSA will follow the FAR Council's guidance, currently under development, for how to respond to certain supply chain events (e.g., breach of Personally Identifiable Information). OGP is developing additional guidance in the GSAM to establish GSA-specific procedures for coordinating and assessing additional supply chain risks on GSA contracts (Case 2021-G511).

[20] The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) is the designated lead for the Quality Services Management Office for cybersecurity and SCRM and is the information sharing agent for the FASC.

Adding C-SCRM to Cloud Services: GSA leads a Government-wide approach to assessing and authorizing cloud service providers through FedRAMP. GSA establishes Government-wide contracts for cloud services and its Centers of Excellence provide modern digital consulting services. Completion of the supplier vetting activities mentioned in Strategic Objective #2 will help to further mitigate supply chain risks on GSA's cloud service offerings. Additionally, FAS is piloting a software security testing technique for select software products. This pilot will be complete in late 2021 and appropriate next steps will be taken following its completion.

Addressing C-SCRM for Drones: GSA IT created an overview of the process by which cybersecurity risks are addressed for small drones used by GSA and by contractors on behalf of GSA.[21] GSA uses drones for internal operations (e.g., PBS land surveys), and the SCRM Executive Board will identify a lead organization to establish necessary SCRM controls (e.g., crash plans) for drones used by, and on behalf of, GSA.

GSA also establishes contracts, which include SCRM requirements, for other agencies to procure drones. GSA will continue to update its drone policy and contract language as needed to respond to new Government-wide guidance, newly-discovered threats, or other supply chain risks. As part of its long-term strategy, FAS has consolidated contracting for the acquisition of drones into a singular region to ensure that knowledge and experience is developed by GSA acquisition professionals overseeing the availability of drones for purchase under the Multiple Award Schedule Program.

Oversight of Plan Effectiveness

Progress on meeting the objectives outlined in this plan will be reviewed quarterly by the SCRM Executive Board. The SCRM Executive Board will also periodically review and consider revisions to the plan itself.

[21] IT Security Procedural Guide: Drones/Unmanned Aircraft Systems (UAS) Security (CIO-IT Security-20-104) (Dec. 26, 2019).

Appendix A: Roles and Responsibilities

The following table describes, at a high level, key positional and organizational roles and responsibilities for each of GSA's major Service and Staff Offices. Some functions are a shared responsibility while other functions fall within the scope of a single office. While the table describes roles and functions pertinent to specific organizations, performing SCRM requires multi-disciplinary, cross-organizational engagement and teamwork.

SCRM Executive Board (including its Working Groups)	- Provide leadership and oversight of SCRM implementation and effectiveness at GSA - Provide oversight and promote coordination and consistency to ensure a harmonized approach for SCRM activities GSA-wide - Provide direction and decisions for SCRM priorities, high-risk issues, and resourcing of SCRM activities - Prioritize and develop SCRM policies and processes
Mission/Business Owners (All Service and Staff Offices)	- Determine risk tolerance level, meet SCRM requirements, and implement controls, based upon criticality analysis of mission functions and assets within the office's span of control and accountability - Perform risk assessments for the office's procurements - Make risk-based decisions in accordance with IT system "authority-to-operate" responsibilities
Office of Government-wide Policy (OGP)	- Lead for creating and updating of GSA's SCRM acquisition policies - Support enabling and improving Government-wide SCRM - Support the development and promulgation of Government-wide SCRM policies and guidance - Support SCRM-related training and development for the civilian acquisition workforce - Provide leadership and support to help ensure Government-wide shared services are incorporating SCRM considerations into program and customer-support functions, outsourced support services contracts, and system controls - Represent GSA to policy-related Government-wide SCRM working groups
GSA IT (including the Chief Information Officer, the Chief Information Security Officer,	- Life cycle management of GSA's information and operational technology systems and assets in accordance with the cybersecurity and risk management frameworks - Assurance of the confidentiality, integrity, and availability of GSA technical infrastructure and assets - Develop and promulgate policies related to cyber and supply chain security for GSA IT systems

and the Chief Privacy Officer)	- Integrate SCRM considerations into ICT procurement and Federal Information Technology Acquisition Reform Act (FITARA) processes - Monitor and report threats and vulnerabilities for GSA IT systems - Oversight of Federal Information Security Modernization Act of 2014 (FISMA) compliance - Establish policies to coordinate C-SCRM incident response for GSA IT systems - Perform supply chain risk assessments for GSA IT systems and acquisitions - Establish and serve as GSA-lead for development, implementation, and ongoing operational management of Tier 3 level C-SCRM policies, plan(s), processes, and controls
Office of the Chief Financial Officer	- Lead incorporation of SCRM into Enterprise Risk Management processes and governance - Provide guidance and support for SCRM-related budget/resource planning and funds allocation - Assist with the development, tracking, and reporting of Enterprise-level SCRM implementation progress and performance metrics
Office of Administrative Services (OAS)	- Integrate SCRM considerations into OAS' customer relationship and acquisition processes - Develop, execute, and provide oversight of OAS' Tier 2 C-SCRM Plan - Work in partnership with GSA IT, OGP, and OMA to ensure the cyber and supply chain security of OAS-managed ICT-related programs and services
Federal Acquisition Service (FAS)	- Represent GSA on the FASC and the FASC Information Sharing Task Force - Develop, execute, and provide oversight of FAS' Tier 2 C-SCRM Plan, integrating SCRM considerations into FAS' customer relationships, and including how to identify critical risks in each of FAS' business offerings, including shared services, assisted acquisition, and acquisition vehicles and how to conduct risk assessments, risk response, and monitoring and control throughout the FAS acquisition lifecycle of each service offering - Work in partnership with GSA IT, OGP, and OMA to ensure the cyber and supply chain security of FAS-managed ICT-related programs, systems, services, and customer-facing shared services
Public Buildings Service (PBS)	- Develop, execute, and provide oversight of PBS' Tier 2 C-SCRM Plan, integrating SCRM considerations into PBS' customer relationships, including how to identify critical risks in

	each of PBS' business offerings, including shared services, assisted acquisition, and acquisition vehicles and how to conduct risk assessments, risk response, and monitoring and control throughout the PBS acquisition lifecycle of each service offering - Work in partnership with GSA IT, OGP, and OMA to ensure the cyber and supply chain security of PBS-managed ICT-related programs, systems, services, and customer-facing shared services
Office of Mission Assurance (OMA)	- Lead GSA's insider threat program, including monitoring, reporting, and remediation - Provide personnel security and physical security of facilities - Liaise between GSA and the Intelligence Community and Law Enforcement - Provide classified communications support - Incorporate SCRM considerations into emergency and contingency plans - Represent GSA's interests and equities to the National Security Council - Co-sector agency for Government Facilities Critical Infrastructure, including addressing cyber and supply chain risks and participating in intragovernmental processes to address cross-sector risks and C-SCRM incident response - Coordinate Committee on Foreign Investment in the United States (CFIUS) case review, assessment, and response
Office of General Counsel	- Provide legal support for GSA SCRM-related efforts, including reviewing processes and documents for legal sufficiency and compliance with relevant laws and regulations - Represent GSA's legal interests, concerns, and positions
Office of Congressional and Intergovernmental Affairs	- Monitor cybersecurity and supply chain related legislation and facilitate internal situational awareness - Communicate GSA's SCRM efforts, as appropriate, to inform and respond to congressional interests and inquiries - Provide guidance and support for SCRM matters involving external Government bodies and officials
Office of Strategic Communications	- Ensure GSA's value proposition in terms of SCRM is clearly communicated to external stakeholders